智能网联汽车数据安全合规白皮书

路特斯科技与普华永道联合发布

LOTUS NYO

pwc 普华永道

声明

- 本白皮书由普华永道商务咨询（上海）有限公司和武汉路特斯科技科技有限公司（以下简称“路特斯科技”）分别撰写。普华永道系指普华永道网络及/或普华永道网络中各自独立的成员机构。详情请进入www.pwc.com/structure。普华永道商务咨询（上海）有限公司负责第一章、第二章和第四章内容，该部分内容从智能网联汽车行业角度出发，结合各国法律法规要求，阐述数据安全合规要求及行业展望；路特斯科技负责第三章内容，该部分从路特斯科技自身实践出发，阐述路特斯科技数据安全合规实践。文中所有文字、数据、图片、表格，均受中华人民共和国著作权法和其它法律法规保护。未经普华永道和路特斯科技书面许可，任何机构和个人不得基于任何商业目的使用本文中的信息（包含本文全部或部分内容）。如果任何机构和个人因非商业、非盈利、非广告的目的需要引用本文中内容，需要注明”转载自普华永道商务咨询（上海）有限公司和武汉路特斯科技有限公司联合发布的《智能网联汽车数据安全合规白皮书》“。
- 本文的信息来源于本次白皮书撰写所收集的数据及公开的资料，对于信息的完整性、准确性和可靠性不做任何保证，在不同时期可能会得出与本文不一致的观点。
- 本文仅供一般参考使用，不构成具体事项和咨询意见，普华永道商务咨询（上海）有限公司不对本文内容承担审慎责任，并且未就本白皮书内容做出任何明示或暗示保证。普华永道商务咨询（上海）有限公司不就本文内容向任何人士承担责任或义务，也不向任何人士承担因本白皮书引起的或与白皮书有关的任何责任或义务。读者不应依赖本文内容做出任何投资或其他商业决定。如需具体意见，请咨询专业顾问。
- 本文中由路特斯科技负责撰写的内容陈述了路特斯科技在发布日期的服务及实践，该部分内容均依据路特斯科技现状提供，不包含任何明示或暗示的保证。该部分信息后续如有变化不会做另行通知，读者对于该部分信息及路特斯科技产品或服务应自己做出独立判断。本部分内容不构成路特斯科技与读者之间的任何协议组成部分，也不构成对任何协议的修改。

目录

第一章

概述

本章围绕智能网联汽车的行业背景及监管体系，介绍了中国、欧盟、美国、英国及国际组织近年来发布的智能网联汽车行业相关的数据安全合规要求。

1.1 智能网联汽车数据安全合规行业背景

随着车联网及人工智能技术的日益成熟及商业化，智能网联汽车（Intelligent Connected Vehicle，简称“ICV”）应运而生。智能网联汽车兼具智能与联网的特性，通过V2X（Vehicle to Everything）通信技术实现了车辆与车辆、人、道路交通设施、云之间的成熟交互。智能网联汽车不仅能进行数据交互和信息共享，优化驾驶路径并降低交通事故发生的风险，还能实现通过传感设备进行自动驾驶等功能，提供个性化的用户体验，引发对未来驾驶方式的展望。

近年来，汽车企业和互联网企业蓬勃发展，加速了车联网、自动驾驶、互联网地图、智能交通技术的升级与革新，世界各国家地区政府对智能网联汽车的大力支持和消费者对出行方式的需求转变，推动了智能网联汽车的研发、生产与普及，商用场景正在不断增加。

为提供更好的用户体验，智能网联汽车及其后台支持系统每时每刻都在处理海量数据，包括车辆运行数据、路况信息、位置信息、车载应用操作信息等。

对于这些数据信息，如果没有严格的数据安全合规管控措施，处理这些数据极易造成安全合规隐患，对国家、公共安全、企业经营、个人隐私等产生影响。

因此，智能网联汽车的数据安全合规在数据生命周期中至关重要，数据安全合规也成为智能网联汽车产业健康发展的重要基础。

随着监管与消费者对数据安全和隐私保护关注程度的提升，全球各国家与地区对于数据安全的法律法规相继出台，针对智能网联汽车的行业规范也在逐步完善。

1.2 各国法律法规和行业规范

中国出台了各项法律法规标准要求，建立数据安全法律保障体系屏障，针对智能网联汽车的数据安全行业规范也在不断完善与深化。

2017年6月1日
《网络安全法》生效

2020年10月1日
YD/T 3746—2020《车联网信息服务 用户个人信息保护要求》、YD/T 3751-2020《车联网信息服务数据安全技术要求》、YD/T 3752-2020《车联网信息服务平台安全防护技术要求》生效

- 发挥了国家标准在智能网联汽车产业生态环境构建中的引领作用，完善了行业数据安全标准规范
- 从数据传输的保密性、数据加密、数据访问规则、动态脱敏、数据销毁等方面，提出层层保护用户数据，保护用户的知情权和选择权，保障智能网联汽车加快创新和安全应用的要求

2021年8月24日
《智能网联汽车 数据通用要求（征求意见稿）》发布

2021年9月1日
《数据安全法》生效

2021年10月1日
《汽车数据安全管理若干规定（试行）》生效

- 提出了对智能网联汽车数据应进行分类分级的要求，需要区分个人信息、座舱数据、车外数据、位置轨迹数据等数据类型，并应相应地配置安全保护措施
- 提出了每年应进行风险评估和数据安全管理情况的常态化报送，形成数据安全保障体系

2021年11月1日
《个人信息保护法》生效

- 确立了“告知-知情-同意”的个人信息处理规则
- 对处理敏感个人信息进行了要求
- 强调了掌握海量用户数据后，互联网平台的“守门人”责任

2022年9月1日
《数据出境安全评估申报指南（第一版）》生效

2022年9月1日
《数据出境安全评估办法》生效

- 要求企业在开展数据出境活动前申报并通过数据出境安全评估
- 对数据出境数量的判断情形作了明确的定义

2023年5月1日
GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》生效

图1 - 中国智能网联汽车数据安全相关重点法律法规和行业规范

放眼全球，为强化智能网联汽车数据安全，保障数据安全和用户隐私，世界各国家与地区也同时在不断强化数据安全合规管理相应的法律法规和行业规范要求。

2013年（2022年更新）
ISO/IEC 27001 信息安全管理体系 发布

2014年（2019年更新）
ISO/IEC 27018 公有云个人可识别信息保护认证 发布

2017年8月6日
《联网和自动驾驶车辆网络安全重要原则》 发布

- 提出保障数据存储和传输安全可控等在内的八大原则
- 强调数据安全问题应纳入汽车生命周期

2017年9月7日
H.R. 3388 《自动驾驶法案》 提出

- 自动驾驶车辆厂商制定网络安全政策
- 要求车辆厂商建立监控、测试和保护关键控制系统的安全机制

2018年5月23日
《2018数据保护法案》 颁布

- 采用了大量GDPR的核心理念
- 提出故意或过失识别出已去识别化的个人数据会构成新的刑事犯罪

2018年5月25日
《通用数据保护条例》(GDPR) 生效

- 定义了个人数据和特殊类别的个人数据
- 提出了个人数据处理需遵循的透明性、数据最小化、完整性与保密性等原则

2019年8月
ISO/IEC 27701 隐私信息管理体系 发布

2020年1月1日
《加州消费者隐私法案》（CCPA） 生效

- 强调加州消费者提供各种与个人信息相关的权利，包括访问权、删除权等

2021年1月12日
《现代车辆安全性的网络安全最佳实践》 发布

- 从整个汽车行业的角度给出了45个重要的原则
- 对网络安全问题提供了解决方案和实践指南

2021年3月9日
《车联网个人数据保护指南 v2.0》 生效

- 将GDPR应用于联网车辆中涉及处理个人数据的场景
- 设定了针对网联汽车数据的基本性保护规则
- 对数据出境进行了规定

2021年4月13日
《自动与电动汽车法案》 生效

- 明确了充电点相关的数据传输等规则

2021年6月28日
《网络安全法案》 生效

- 规定个人信息保护要求

2021年8月31日
ISO/SAE 21434: 2021 《道路车辆-信息安全工程》 发布

2022年6月21日
《美国数据隐私和保护法案》 发布

- 在隐私政策中要求披露收集的数据类型、处理目的、与第三方共享数据的情况

2022年7月6日
《网络安全管理系统》(UN R155)
《软件更新管理系统》(UN R156)
生效

- 由联合国世界车辆法律协调论坛（WP.29）发布的全球第一个汽车信息安全强制性法规
- R155要求汽车制造商在车辆生命周期的各阶段制定网络安全管理流程
- R156是关于软件更新和软件升级管理体系车辆审批的统一规定
- 在欧盟汽车组提交的修订案中，UN R155和UN R156共同成为防护车辆网络攻击的技术法规

2023年1月1日
《加利福尼亚隐私权法案》(CPRA, CCPA修正版) 生效

图2 - 海外各国家与地区智能网联汽车数据安全相关重点法律法规和行业规范

世界各地对智能网联汽车数据安全合规领域均提出了**采取适当的技术和组织措施来保护数据的机密性、完整性和可用性，保护个人信息，以及在适当的情况下获得消费者同意的要求。**但在不同的国家和地区，具体的要求内容存在差异：

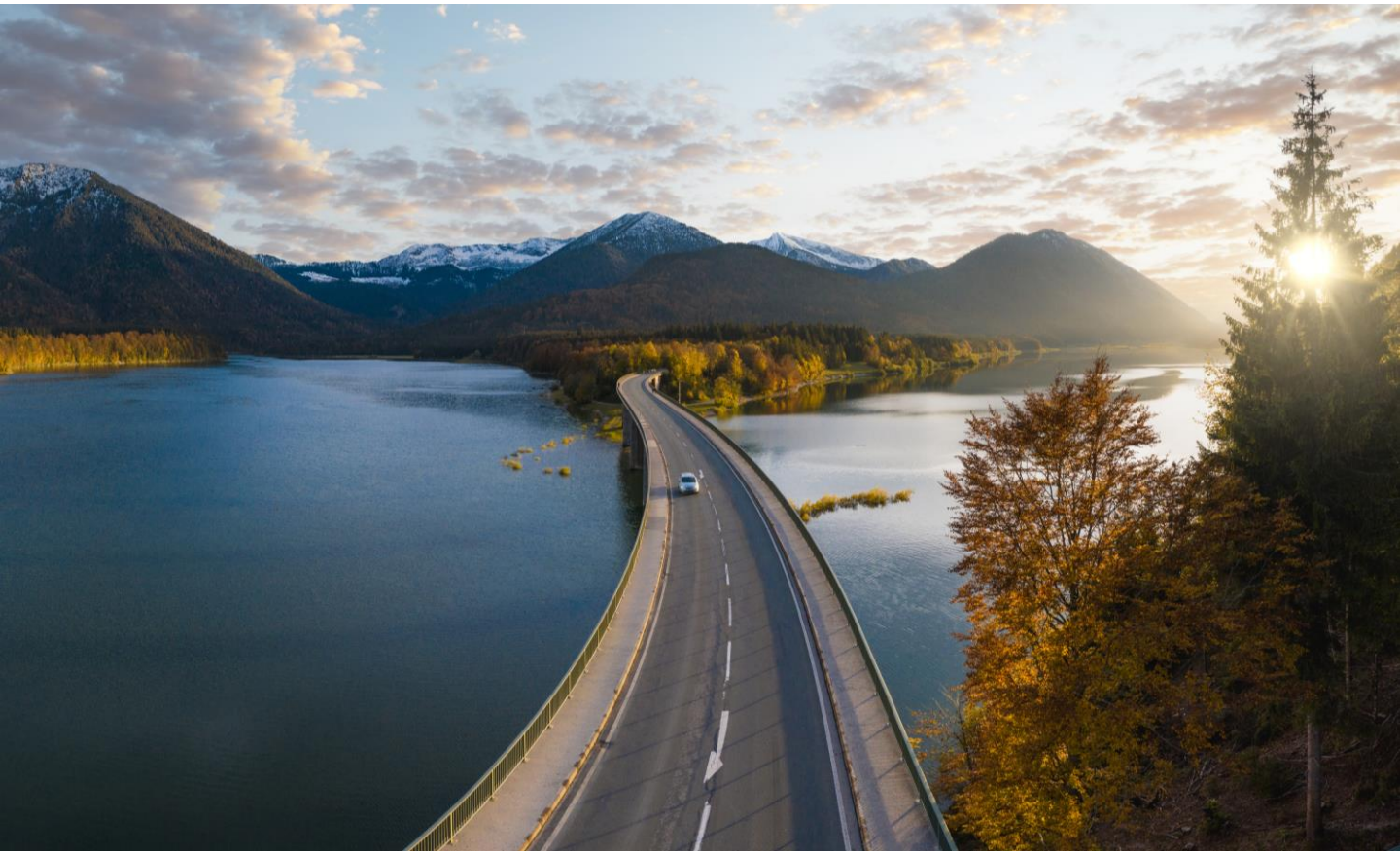
个人信息分类：

欧盟强调个人数据的特殊类别，在GDPR中有明确的定义，而美国对敏感个人信息的定义因法律法规不同而有差异。

汽车数据安全：

中国出台行业规范，英美提出原则和最佳实践，欧盟重点关注该场景下的个人信息保护，后续可能在联合国世界车辆法规协调论坛（WP.29）对不同系统继续发布安全合规要求。

智能网联汽车生态伙伴需在满足行业通用标准的基础上，在各地区经营时，遵守当地相关法律法规和行业规范。



第二章

智能网联汽车数据安全合规要求及建议

本章依据行业规范及要求，梳理了智能网联汽车数据分类分级、数据生命周期的安全合规要求，并对智能网联汽车数据安全合规实践提出建议。

2.1 智能网联汽车数据分类分级

数据是驱动智能网联汽车发展的重要资产，合理的数据分类分级是妥善管理数据的基础，也是海量数据处理的基础。为实现智能网联汽车数据在数据生命周期的安全治理，应根据科学合理、客观明确的原则对相关数据进行分类分级。本白皮书将依据已发布的行业规范要求，从**个人信息**和**车辆数据**角度对智能网联车数据的安全合规要求展开分析。

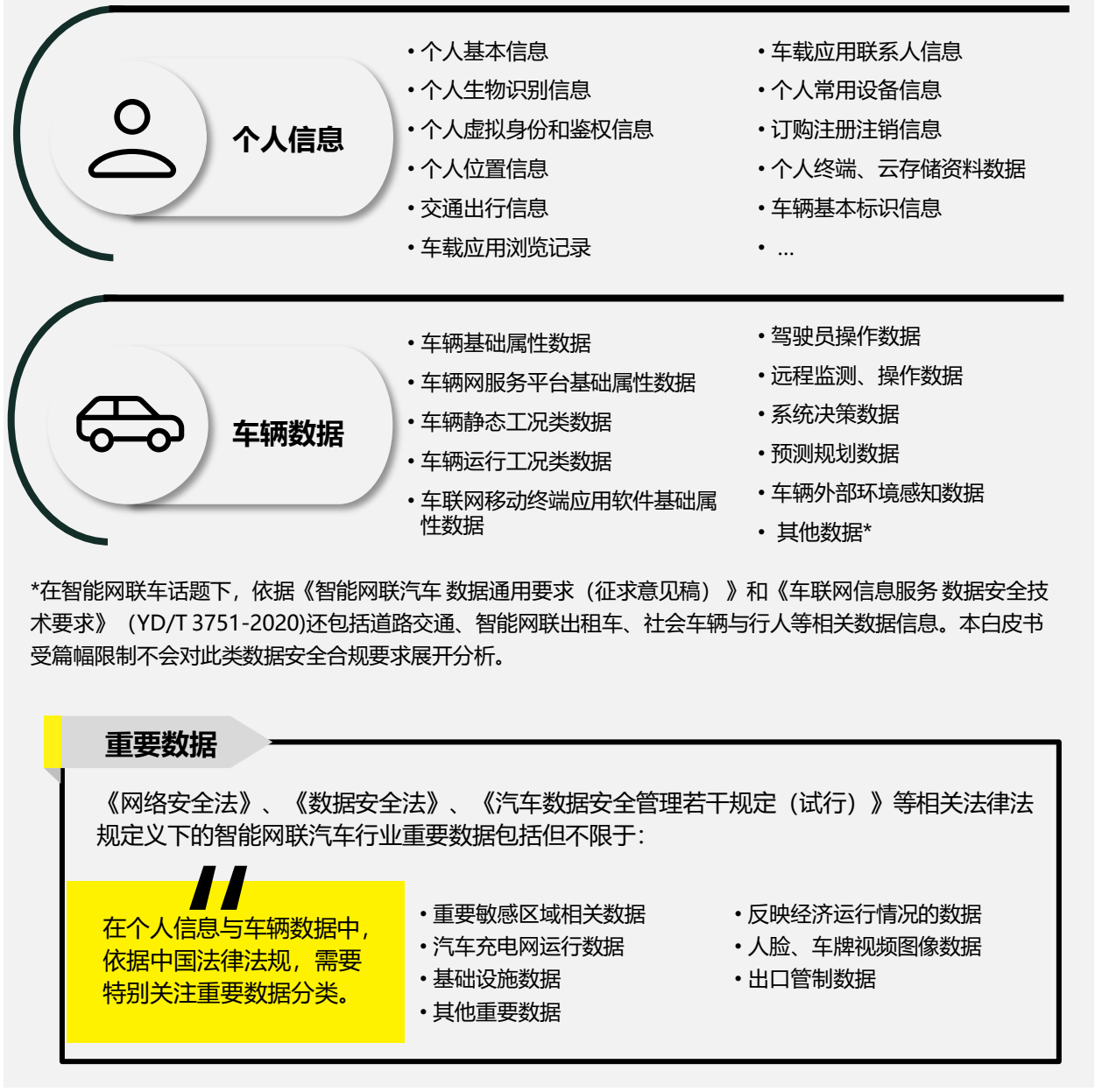


图3 - 智能网联汽车数据分类示例

在数据分类的基础上，根据数据发生安全问题时的影响对象和影响程度，可进一步将不同数据分为**一般级**、**敏感级**、**重要级**和**核心级**（见图4）。

一般级

- 指在被泄露、篡改、破坏或非法获取、非法利用、非法共享后，会对用户或企业合法权益造成一般危害的数据

敏感级

- 指在被泄露、篡改、破坏或非法获取、非法利用、非法共享后，会对用户或企业合法权益造成较大危害的数据

重要级

- 指在被泄露、篡改、破坏或非法获取、非法利用、非法共享后，会对用户或企业合法权益造成严重危害的数据

核心级

- 指在被泄露、篡改、破坏或非法获取、非法利用、非法共享后，会对公共利益造成严重危害、对国家安全造成一般危害的数据
- 尤其包括图3列示的重要数据

图4 - 智能网联汽车数据分级示例

同一数据由于数据量的累积或使用场景的变化会造成数据级别上升；

不同种类数据的组合、汇聚、分析可能会造成数据级别上升。

因此数据分级可结合实际情况进行划分与调整。

2.2 智能网联汽车数据生命周期合规要求分析

为确保数据生命周期内的数据安全合规，企业需要在数据分类分级的基础上，不断完善自身管理手段和技术措施。在此过程中，保证数据的机密性、完整性及可用性，满足安全合规要求的同时，还应特别关注其中涉及不同类别、不同级别数据处理的特殊要求，如重要数据、个人隐私数据等。

智能网联汽车数据生命周期典型安全合规要求

车内传输：基于车内处理原则，原则上数据应仅在车内传输

车外传输：仅在法定要求或履行合同所必须的情况下进行车外传输，并需要：

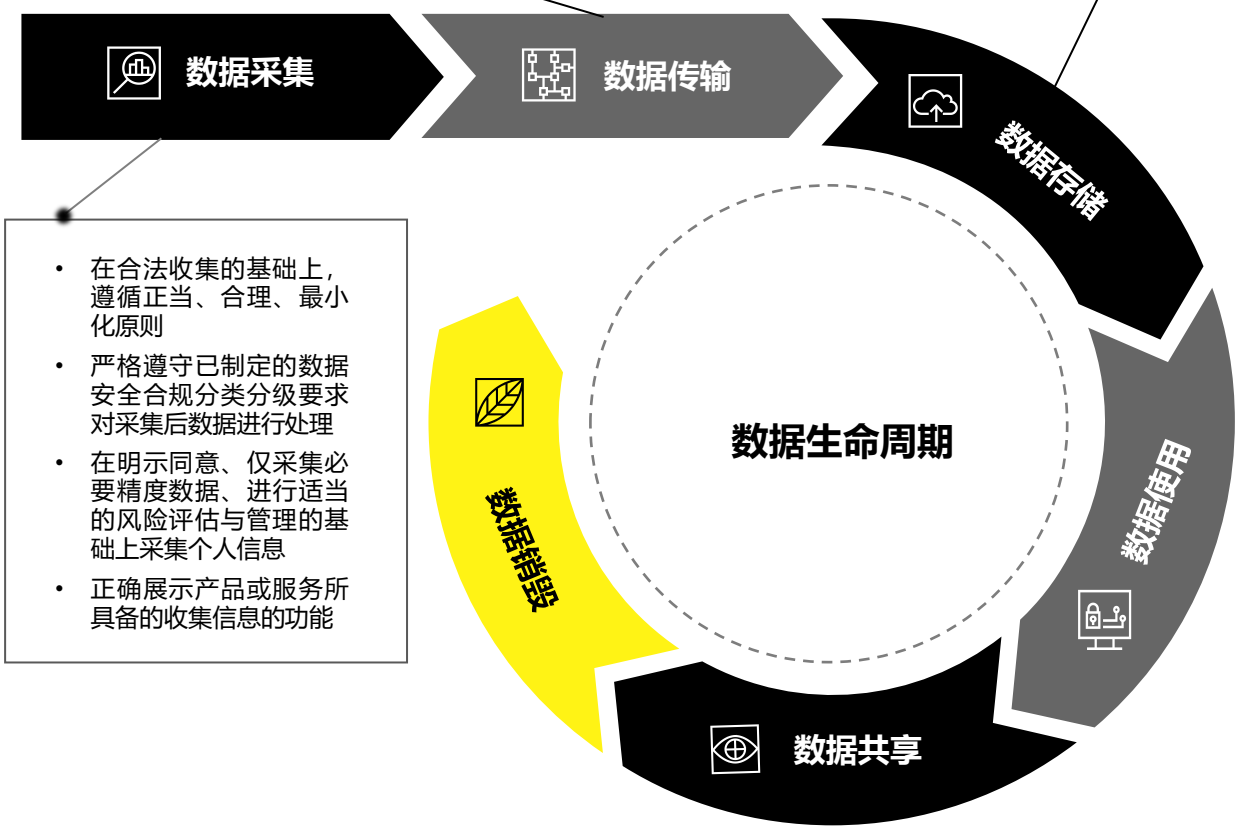
- 获得用户单独同意
- 确保传输后数据仅用于必要的功能
- 在传输前进行必要的脱敏、加密等处理
- 对传输信道进行技术保护
- 严格执行数据权限管控

车内本地存储：应满足事故风险排查及事故数据还原要求

车外存储：仅存储必要数据

本地与车外数据存储均应保证：

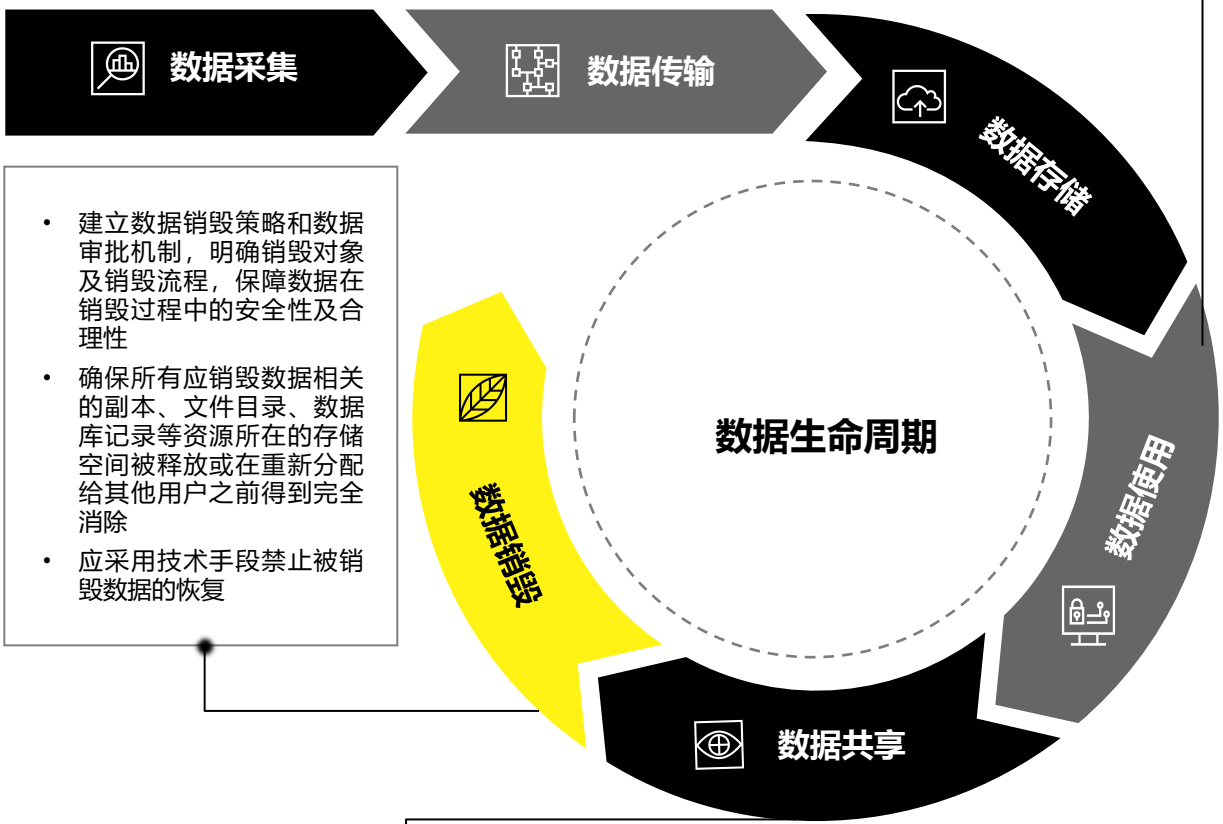
- 采用合理技术手段加密或脱敏存储数据，配置安全控制以防数据被篡改或恶意删除
- 正确配置存储周期，符合监管对存储期限要求



- 在合法收集的基础上，遵循正当、合理、最小化原则
- 严格遵守已制定的数据安全合规分类分级要求对采集后数据进行处理
- 在明示同意、仅采集必要精度数据、进行适当的风险评估与管理的基础上采集个人信息
- 正确展示产品或服务所具备的收集信息的功能

智能网联汽车数据生命周期典型安全合规要求（续）

- 不能影响车辆正常驾驶和行驶安全
- 依据数据分类分级标准对数据的使用进行授权和验证
- 重要数据、个人隐私数据及其他敏感信息的使用需进行脱敏，如使用去标识、匿名化、加密处理等方式
- 对数据使用行为进行审计



- 建立数据销毁策略和数据审批机制，明确销毁对象及销毁流程，保障数据在销毁过程中的安全性及合理性
- 确保所有应销毁数据相关的副本、文件目录、数据库记录等资源所在的存储空间被释放或在重新分配给其他用户之前得到完全消除
- 应采用技术手段禁止被销毁数据的恢复

数据共享：

- 基于充分有效的评估进行数据共享，包括可行性评估、风险评估、网络安全能力评估
- 制定数据共享风险控制措施，以保证数据共享的安全
- 数据接收方同样需要履行数据保护的义务

关于数据出境：

严格判断车外数据、座舱数据、位置数据等相关数据的出境状态

重要数据原则上应当存储在境内，确需向境外提供的，须通过有关部门组织的安全评估，所提供的数据不得超过出境安全评估所定的目的、范围、方式、种类等

2.3 主要市场的数据跨境合规事项

中国

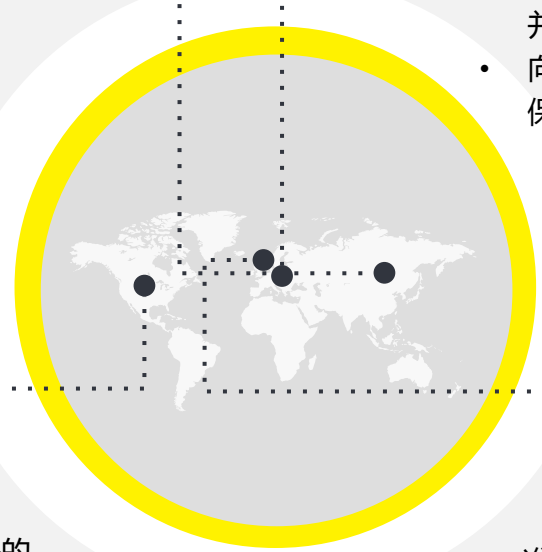
中国重视数据出境安全，不断立法进行强调保护原则。企业需对出境数据进行安全自评估，并根据评估结果，选择采取以下几种措施：

- 向网信部门申请出境数据安全评估
- 采用个人信息出境标准合同规定
- 实施个人信息保护认证

欧盟

在对方国家提供与欧盟同等水平保护措施的前提下，欧洲允许数据跨境流动。通常企业需要采取如下一种保障措施：

- 申请约束性公司规则（BCR）
- 签署标准合同条款（SCC）
- 作出行为准则（CoC）承诺，并向欧盟委员会申请批准
- 向成员国监管机构申请数据保护认证（Certification）



美国

美国主张全球数据自由流动，同时也对企业敏感数据的跨境进行严格的管理，包括：

- 若企业涉及敏感个人数据交易，则需要进行外国投资安全审查
- 评估应用程序风险，确保外国无法访问敏感的个人数据或机密的政府信息、商业信息
- 网络服务提供商应默认向美国政府披露其控制的通信内容等数据

英国

英国根据脱欧后制定的《英国通用数据保护准则》中提出了跨境传输的标准合同要求。标准数据保护条款（UK SCC）涉及两份文件，要求企业选择其一进行签署：

- 国际数据传输协议（IDTA）
- 欧盟委员会标准合同条款国际数据传输附件（IDTA to the EU Commission SCC）

*除上述中国、欧盟、美国、英国外，其他国家地区市场的数据跨境活动也应符合当地相关法律法规要求。

2.4 智能网联汽车数据安全合规实践整体建议

数据安全合规建设，特别是个人隐私保护的合规建设，已成为行业内的重点议题。由于掌握了海量的个人与车辆数据，智能网联汽车企业需要特别关注数据安全与隐私保护风险。

基于已有的法律法规及行业规范的梳理与分析，我们提示以下数据安全合规实践方式，为行业内企业提供参考。

1 明确数据安全与隐私保护合规战略

数据安全与隐私保护合规战略不仅应包括本主题下公司的愿景、使命及目标，还应包括企业对于数据安全合规的承诺，为企业合规框架的建立及后续执行确立方向。

2 建设数据安全合规管理体系，完善合规组织机构建设

法律法规、行业规范与企业要求共同构成了数据生命周期内企业应遵循的规范。建立一套全面、体系化、符合行业业务特性、可落地的安全合规管理体系，有助于推动数据安全在全公司及其关联公司内普及和执行。同时，设计配套的管理制度及组织机构，对于实现有效地管理必不可少。

3 使用默认隐私设计（Privacy by Design）

默认隐私设计（Privacy by Design）的理念可以帮助企业将隐私合规要求与控制融入业务设计、流程制定、产品开发、测试验证及执行监控等全业务流程，为企业提供了开展和执行业务流程相关的隐私合规的方法论。

默认隐私设计是一种隐私保护的方法论，以解决公众对隐私的担忧。默认隐私设计主张将隐私保护前置，即将隐私保护作为系统运行的默认规则，在系统设计的最初阶段纳入隐私和数据保护的需求。根据安·卡沃基发布的《默认隐私设计：七项基本原则》，默认隐私设计应遵循七大原则：

- 积极预防，而非被动救济
- 隐私默认保护
- 将隐私嵌入设计之中
- 功能完整：正和而非零和
- 全生命周期的保护
- 可见性和透明性
- 尊重用户隐私：确保以用户为中心

4 **落实数据生命周期中的安全合规控制**

在生命周期的每一个环节，企业都应当建立并尽可能系统化实施适当的合规流程控制，将合规作为“背景工作”：既提供足够的重视，而又尽可能减少其对业务效率的影响。

5 **有效的披露与展示**

在完成数据安全合规的建设、推广与落地之外，我们同样提倡企业就面向社会、面向消费者最关心的数据安全与隐私保护问题进行有效的披露与展示。

第三章

路特斯科技
数据安全合规实践

本章介绍了路特斯科技在智能网联汽车领域的数据安全合规实践经验，包括路特斯科技数据安全合规战略愿景及数据安全合规实践展示。

3.1 战略与愿景

3.1.1 数据安全与隐私保护战略愿景概述

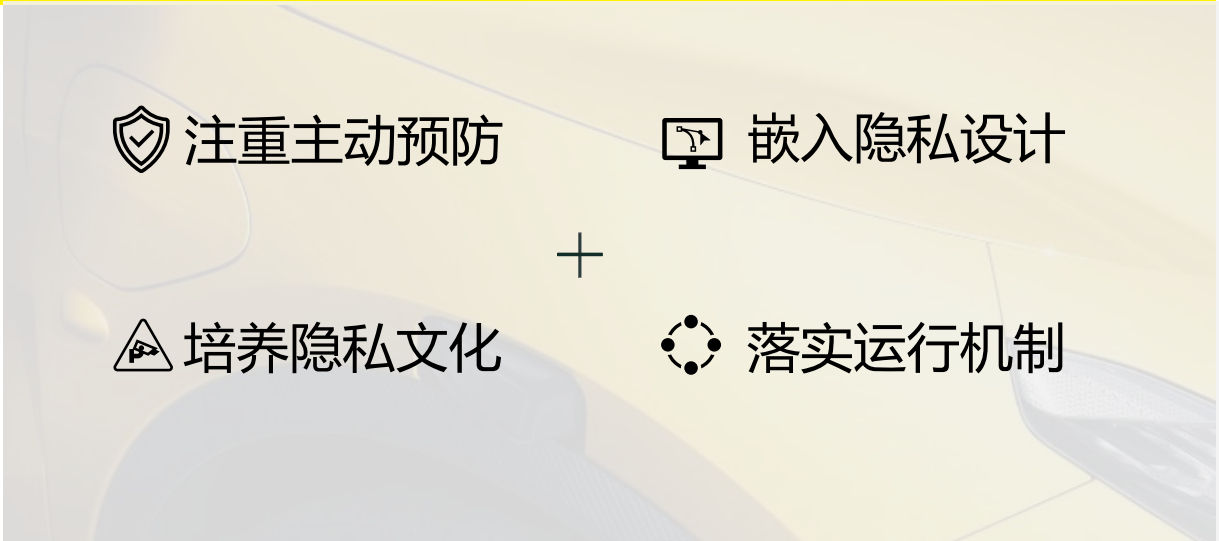
战略愿景

“从F1赛道驶向电气化未来，在路特斯品牌夺冠信念的引领下，为客户提供安全可靠的数据安全与隐私保护体验。”

为实现数据安全，保护用户隐私，为产品、服务的持续运行提供所需的信息安全保障，路特斯科技制定了“**分级保护、风险管控、持续改进、安全高效、行业领先、用户信赖**”的总体信息安全和数据安全策略。并在此基础上，为更好地保护用户数据，提出以下隐私保护的愿景与方针：

隐私保护愿景

“塑造信任，做智能汽车时代最让公众放心的隐私保护践行者。”



3.1.2 面向用户的隐私保护承诺

路特斯科技重视并致力于保护用户隐私，面向用户承诺：

- 路特斯科技仅在合法、正当、必要的原则下收集用户的信息，并仅在实现数据处理目的必要的期限内存储
- 路特斯科技只会将用户的个人信息用于用户预先同意或者法律法规规定的合法目的
- 路特斯科技通过严格的数据保护措施保护用户的个人信息
- 路特斯科技仅在用户明确同意或法律规定的前提下向第三方提供用户的信息，并持续向用户披露共享信息清单
- 如果发生数据泄露或其他安全事件，路特斯科技会及时通知用户，并采取适当措施来减轻损害
- 路特斯科技尊重用户依法享有的对自身信息处理的权利

3.1.3 已获得的第三方认证及说明

ISO/IEC 27001

ISO/IEC 27001是目前为国际上最为认可的信息安全管理体系标准之一。路特斯科技通过建立ISO/IEC 27001体系和ISO/IEC 27701体系能够从企业内部的管理程序（尤其是信息安全管理和个人信息隐私保护）获得巨大的改善，提升企业在信息安全和隐私保护领域的可靠性，降低企业信息泄露的风险，从而更好地保护企业数据。

CSMS

网络安全管理体系（CSMS）认证是联合国世界车辆法律协调论坛（WP.29）通过的R155法规的合规认证。通过CSMS认证说明了汽车制造商在车辆完整生命周期的各个阶段均制定了网络安全管理流程，能识别潜在风险，持续监控和检测网络攻击及漏洞，及时响应网络安全事件。

SUMS

软件更新管理体系（SUMS）认证是联合国世界车辆法律协调论坛（WP.29）通过的R156法规的合规认证。SUMS认证标志着企业构建的软件开发和运营管理体系符合国际车辆软件升级法规要求，表明了汽车制造商在车辆全生命周期内具备确保软件升级过程安全、可靠、合规的工程能力。

MLPS 2.0

我国实行网络安全等级保护制度（MLPS 2.0），对网络运营者针对不同安全保护等级网络的安全保护义务提出了明确、细化的要求。等级越高，说明信息系统重要性越高。获得网络安全等级保护测评标志着企业在技术服务能力、信息安全管理能力和信息应急保障能力等方面达到了国家信息安全标准，用户的信息安全需求能够得到充分保障。

3.2 数据安全与隐私保护合规实践

3.2.1 数据安全与隐私保护治理框架

为深化企业数据安全与隐私保护战略，路特斯科技基于ISO/IEC管理体系标准，建立了信息安全管理体系（ISMS），并基于数据生命周期展开隐私保护管理体系（PIMS）、网络安全管理体系（CSMS）和软件更新管理体系（SUMS）的建设和完善，形成了路特斯科技独特的数据安全与隐私保护治理框架。

图5 - 数据安全与隐私保护治理框架

3.2.2 数据安全与隐私保护管理体系建设实践

为贯彻执行数据安全与隐私保护管理体系，路特斯科技在已有的信息安全组织架构的基础上，建立了数据安全与隐私保护管理体系组织架构（如图6）。该组织架构包括决策层，管理层，执行层和监督层。

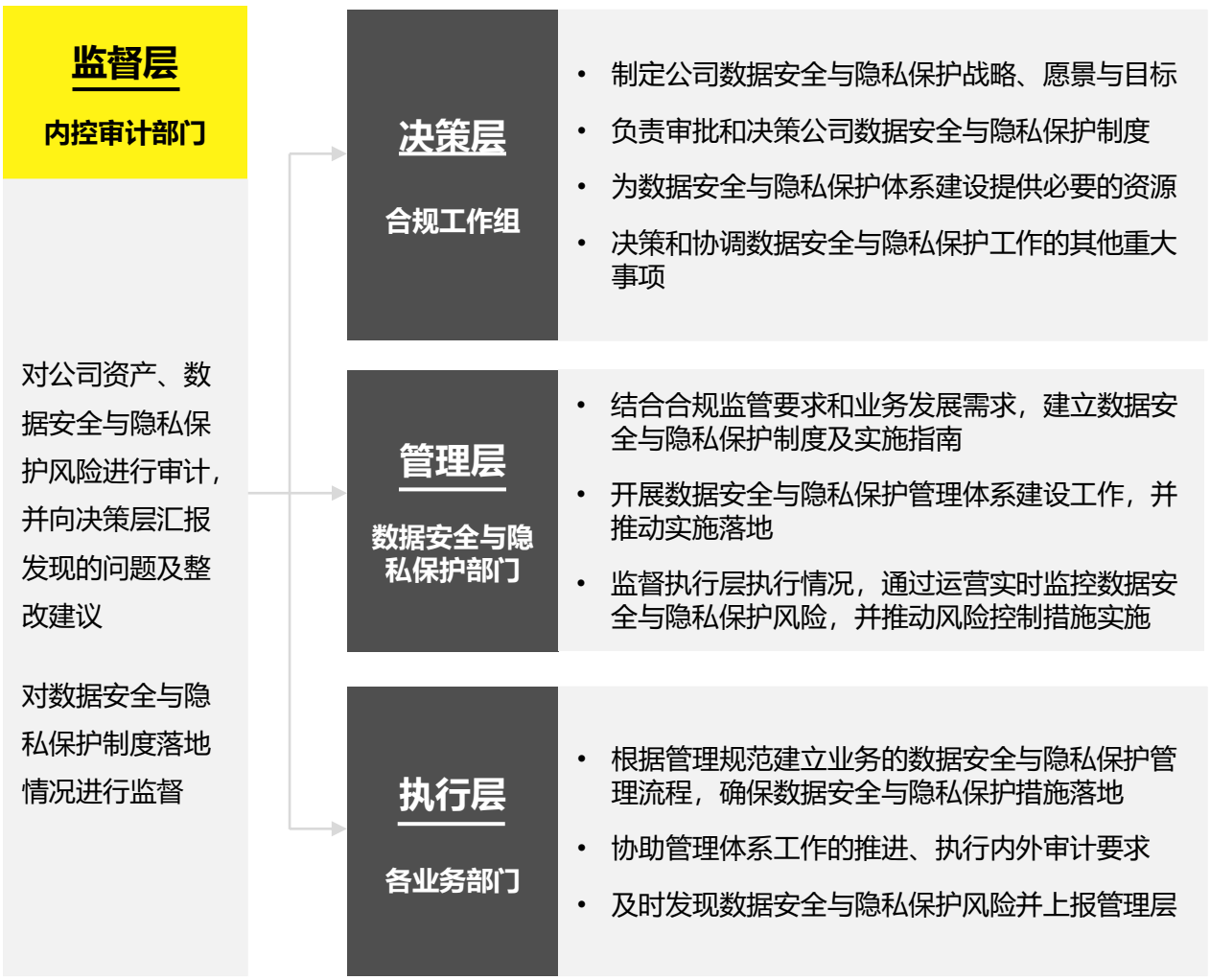


图6 - 路特斯科技数据安全与隐私保护管理体系组织架构

路特斯科技数据安全与隐私保护管理体系组织架构贯彻路特斯科技整体信息安全管理方针、目标，构建了规范高效的数据安全与隐私保护管控体系，提升了数据安全与隐私保护技术能力，实现了数据安全与隐私保护管理体系的有效运行、持续改进。

路特斯科技遵循数据安全与隐私保护管理体系和组织架构，采取以下措施保障数据安全与隐私保护在数据全生命周期过程中的充分性和有效性。

图7- 路特斯科技数据安全与隐私保护合规实践

3.2.3 数据分类分级实践

3.2.3.1 数据分类分级标准

在数据安全与隐私保护治理框架的基础上，路特斯科技制定了相关数据分类分级管理制度，规范企业数据分类分级，并在遵循国家和行业数据分类要求的基础上，从对不同维度的数据类别进行识别，从影响对象、影响程度两个方面综合考虑，将数据分为**一般、敏感、重要、核心**四个级别。

图8 - 路特斯科技数据分类

分类			分级			
父类	一层子类	二层子类	一般	敏感	重要	核心
经营管理数据	战略规划数据	人力需求规划信息			✓	
		品牌战略规划信息			✓	
	招聘数据	招聘岗位信息	✓			
		应聘人员信息			✓	
业务数据	营销数据	门店信息	✓			
		订单信息			✓	
	运营数据	运营分析信息			✓	
		意见反馈信息		✓		
		充电网运营数据				✓
客户数据	个人数据	个人生物识别信息				✓
		个人身份信息			✓	
		个人财产信息			✓	
	车辆数据	车辆标识信息		✓		
		车辆配置信息	✓			

图9 - 路特斯科技数据分类分级示例

3.2.3.2 敏感数据发现系统

根据公司业务涉及的数据特征和分类分级规范，路特斯科技建立了敏感数据发现系统。该系统可通过敏感数据识别技术，全面、快速、准确发现和定位敏感数据，对公司数据进行标识，协助构建完善的企业数据安全管理平台。

01 **数据资产发现**

02 **数据分类分级**

数据分类分级示例

类别	示例	分级
订单数据	• 订单编号 • 订单状态 • 订单数量 • 购车方式	敏感数据
成本数据	• 零部件成本价 • 车辆成本价格	核心数据

03 **敏感数据发现**

敏感数据发现示例

数据特征	是否脱敏	是否加密
纳税人识别号	否	否
字段路径信息		相似度
大数据平台		100% 纳税人识别号

04 **敏感数据目录**

敏感数据目录示例

字段名	数据分类	数据类型
cardid	个人财产信息	账号
trace_time	个人财产信息	交易时间
charge	个人财产信息	刷卡手续费
card_type	个人财产信息	购买人证件类型
id_card	个人身份信息	身份证号

05 **安全风险评估**

图10 - 路特斯科技敏感数据发现系统流程及示例

3.2.4 数据全生命周期安全管理实践

3.2.4.1 数据全生命周期安全策略

在数据分类分级的基础上，为提升数据资产价值，实现企业数字战略，路特斯科技在数据生命周期各环节均采取了相应的安全控制措施，以确保全生命周期数据安全合规。

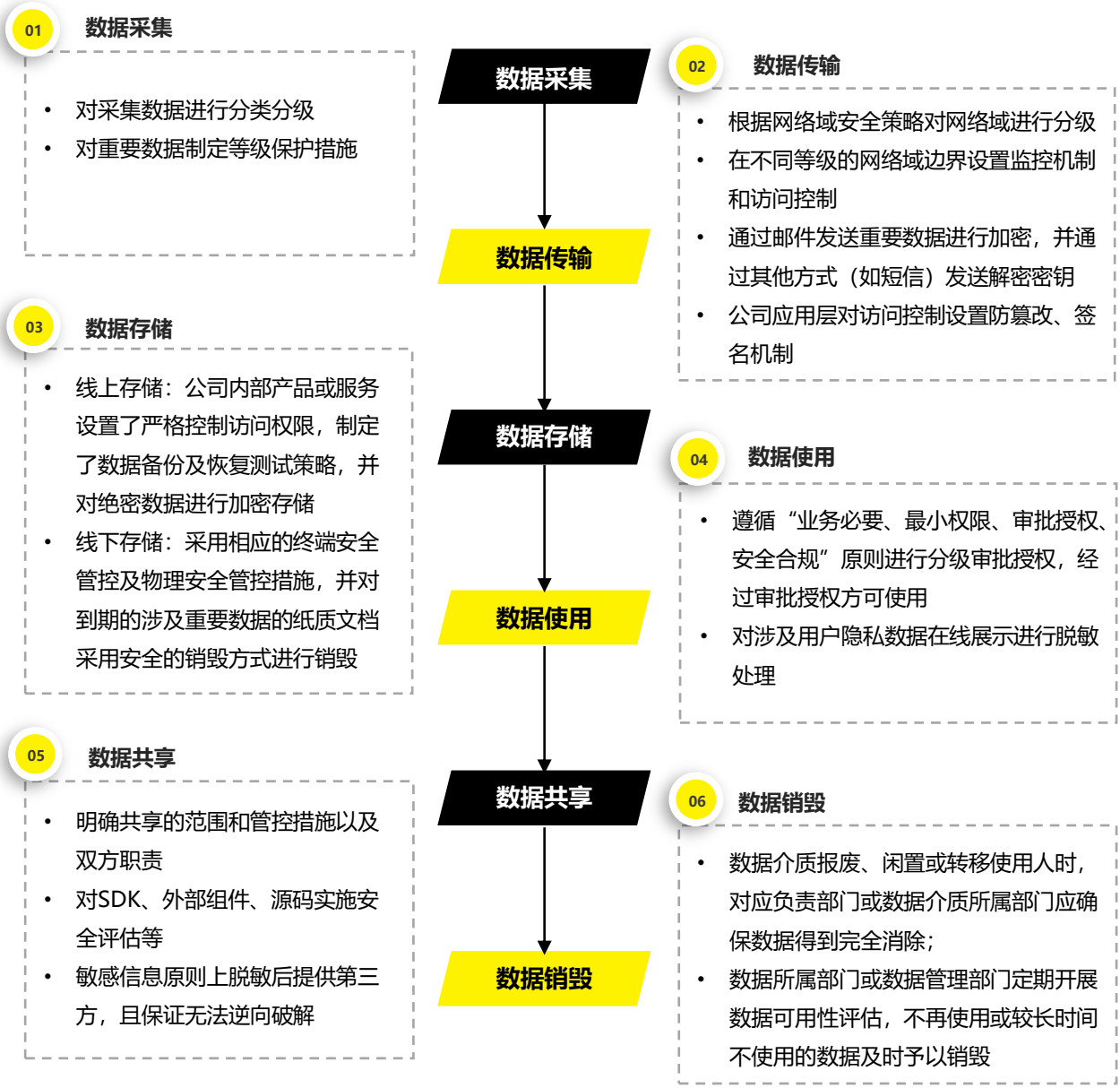


图11 - 路特斯科技数据全生命周期安全控制示例

3.2.4.2 数据全生命周期安全技术架构实践

路特斯科技从数据安全生命周期角度出发，根据管理要求通过技术手段进行全面、系统的数据安全管理管控，实现数据安全目标。在部署通用技术工具的基础上，针对数据安全生命周期的各个阶段，采取相应的安全技术保障。

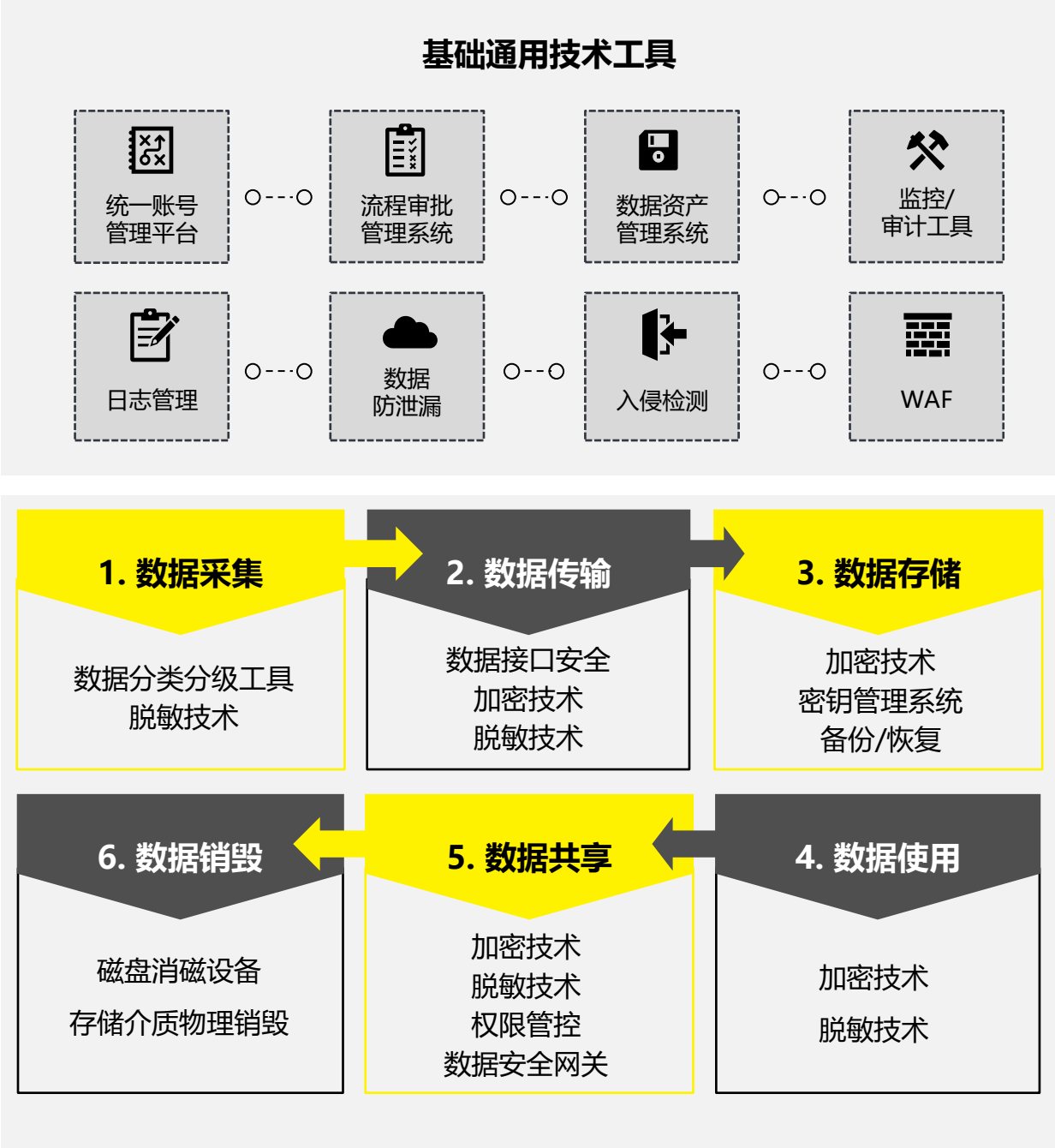


图12 - 路特斯科技数据全生命周期安全技术架构实践示例

3.2.5 隐私保护影响评估实践

隐私保护影响评估是路特斯科技隐私合规实践的核心。路特斯科技设计并实践了如下的个人信息收集与处理控制影响评估流程，来开展全面的个人信息保护影响评估活动（PIPIA）。

预评估PIPIA触发标准示例：

- 是否涉及处理个人信息或个人敏感信息
- 是否涉及公共区域的监测
- 是否涉及对个人进行分析、监控、评估等
- 是否涉及自动化决策
- 是否会阻止个人信息主体行使权利、使用服务或履行合同
- 是否大规模处理个人信息
- 是否向境外提供个人信息

数据处理活动分析动作示例：

- 明确个人信息处理活动的基本信息
- 明确个人信息收集的方式
- 针对个人信息收集采取的控制措施
- 明确个人信息保留期限、个人信息删除/去标识化等信息
- 明确针对个人信息采取的安全措施
- 明确个人信息主体可享有的权利及对应的响应时间、响应流程

风险应对措施执行示例：

- 采用隐私政策、授权条款等方式告知个人信息处理方式
- 向用户明确告知需要披露的信息
- 在隐私政策中向个人信息主体告知处理者的名称和联系方式
- 提供用户撤回授权渠道
- 及时更新隐私政策, 并重新取得用户同意
- 确保收集的是为实现业务目的所必须的最少的个人信息
- 采用表单和后端的验证机制检验个人的真实性和准确性

3.2.6 默认隐私设计（PbD）

路特斯科技在隐私保护设计中，参照默认隐私设计（PbD）的理念及行业最佳实践，将数据安全与隐私保护融入到产品生命周期的各个环节，以求主动识别产品的隐私设计缺陷，预防隐私漏洞，并在负面影响发生之前进行主动、全面的修正。

需求评审

在产品需求设计阶段，由业务需求方主导，数据安全与隐私保护管理部门共同参与，对产品进行安全隐私需求分析和风险评估。

安全隐私设计

进入设计阶段，数据安全与隐私保护管理部门对需要缓解的风险进行隐私保护设计，这一需求将和产品安全需求整合，形成最终产品安全隐私设计文档。

安全隐私开发

开发团队进行组件单元开发（软件，硬件等），以实现安全隐私需求。

发布评审

由业务主导的产品发布评审，审核设计结果能否满足前期制定的安全隐私需求目标（即降低安全合规风险）。

安全隐私测试

根据测试验证结果，由数据安全与隐私保护管理部门确认产品开发满足设计阶段制定的安全隐私需求。

3.2.7 用户数据主体权利（DSR）保障实践

隐私保护影响评估是路特斯科技隐私合规实践的核心。路特斯科技设计并实践了如下的个人信息收集与处理控制影响评估流程，来开展全面的个人信息保护影响评估活动（PIPIA）。

图13 - 用户数据主体权利（DSR）保障实践示例

3.2.8 路特斯科技全球化数据架构实践

基于路特斯科技全球化战略，路特斯科技的产品在保证全球市场产品一致性的同时，也为满足各地区和国家数据跨境及数据本地化存储的合规要求，路特斯科技建立了全球数据中心架构布局。路特斯科技在全球已建立或规划五个数据中心，分别位于中国、德国、美国、新加坡和阿联酋。

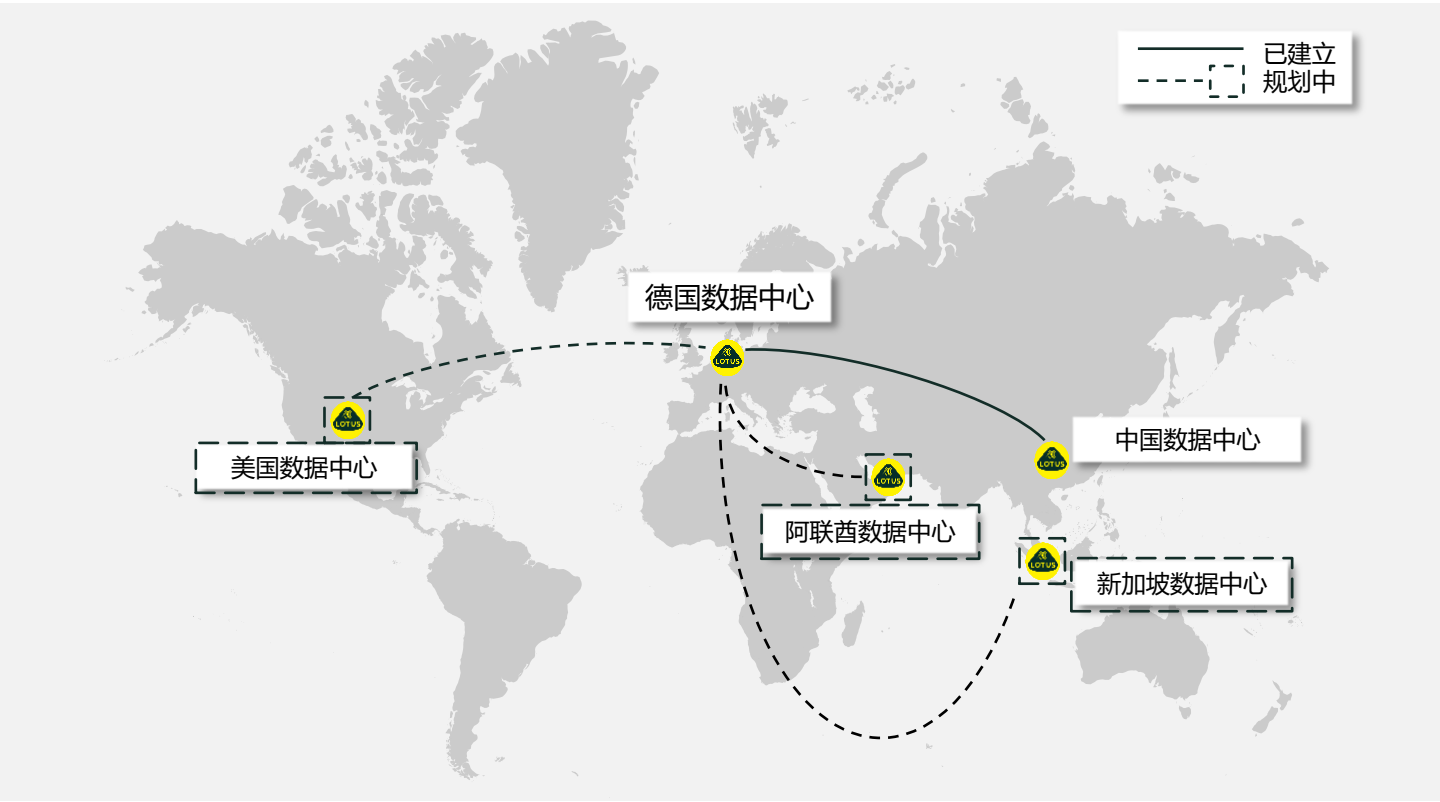


图14 - 路特斯科技全球化数据中心架构布局

3.2.9 路特斯科技数据跨境传输合规实践

针对数据跨境场景，路特斯制定了明确的数据跨境传输流程，以保障企业数据跨境活动符合全球不同司法辖区的基本要求。

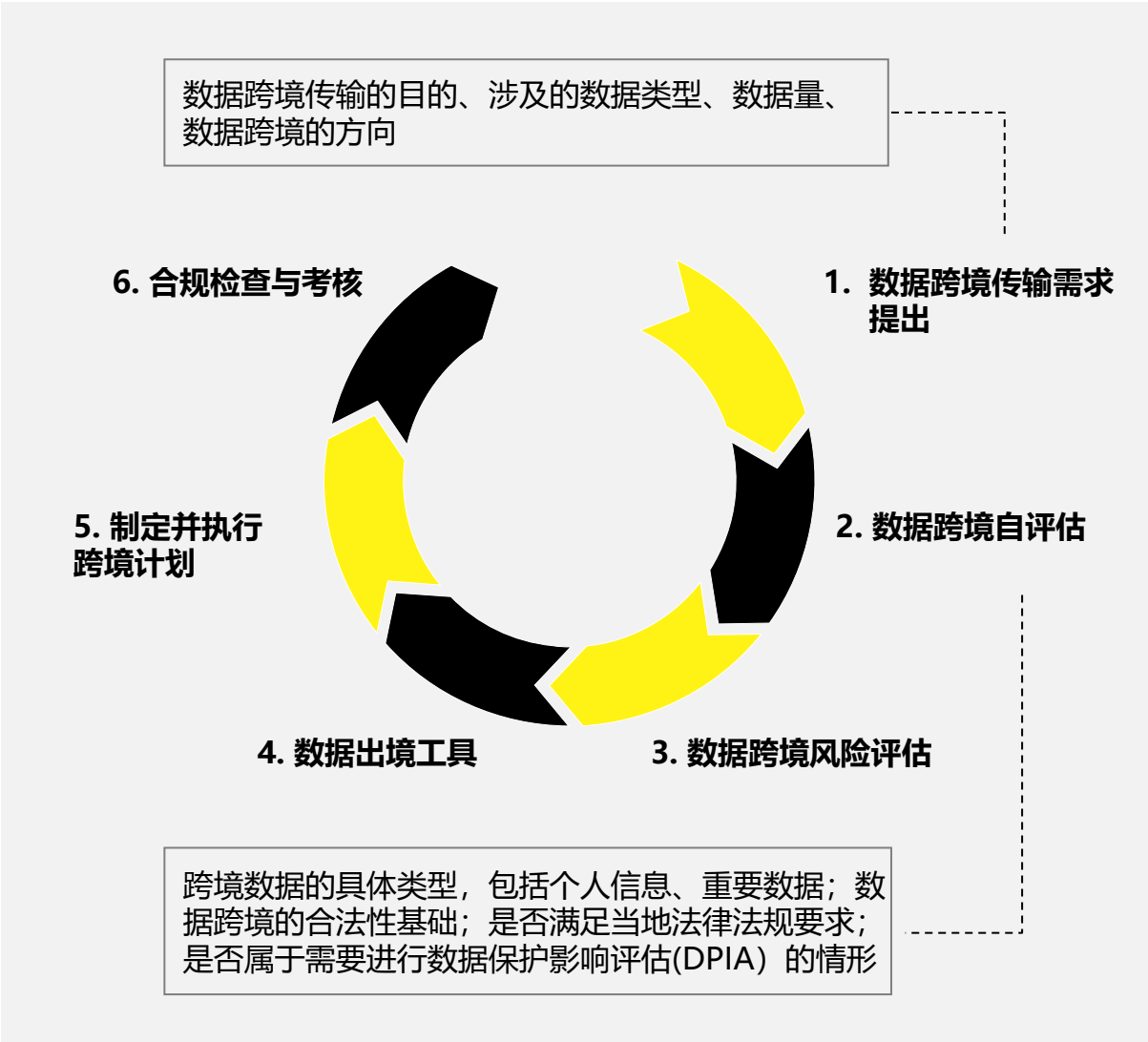


图15 - 路特斯科技数据跨境传输合规实践示意

3.2.10 智能网联汽车隐私保护实践

显著告知 / 用户同意

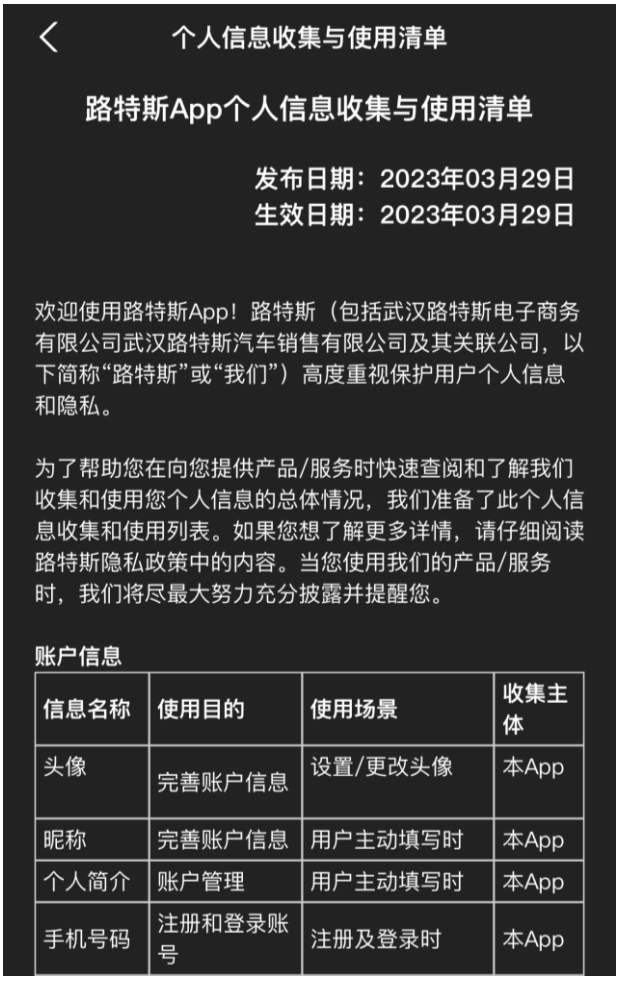


图16 - 路特斯科技个人信息收集与使用清单页面

图17 - 路特斯科技隐私与权限设置页面

单独同意 / 持续披露

视频、图像匿名化处理

- 量产车车端已集成脱敏软件，所有数据上传云端前已进行脱敏处理
- 处理方法为针对人脸与车牌进行不可复原的色块遮盖

匿名化处理流程	匿名化处理各阶段输出
车内数据 - 采集及本地脱敏处理	
1. 获取图像及视频信息	原始图像及视频
2. 分析图像并识别敏感数据	原始图像及视频的敏感数据
3. 判定敏感数据所在图像区域	敏感数据区域脱敏处理标记
4. 回传脱敏后的图像及视频信息	完成脱敏处理后的回传数据
车外数据 - 通过安全信道回传云端	
5. 云端仅存储脱敏后的数据	脱敏处理后的回传数据

图18 - 路特斯科技图像匿名化处理展示

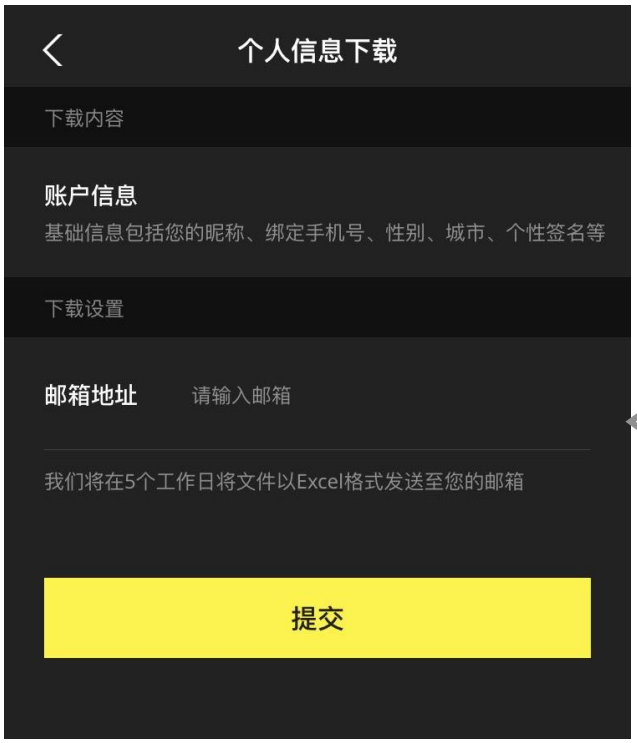
敏感信息单独同意

- 针对语音和人脸的信息收集，单独向用户进行授权请求，并选择授权期限（单次有效/12个月有效）
- 针对地理位置的信息收集，单独向用户进行授权请求，并可以选择授权期限（单次有效/12个月有效）

座舱数据默认车内处理

- 语音助手只识别开关信息，执行相应指令，原音频文件14天自动销毁
- 座椅、方向盘等用户偏好数据不会上传至云端
- 行车记录仪采集的车外视频信息不会上传至云端
- 仅在业务必须，且获得用户授权同意后，可向车外传输，并在功能实现后删除原始数据及处理结果

图19 - 路特斯科技隐私文案交互页面



个人主体权利

用户数据主体享有对其个人数据的查阅权。考虑到用户权利，为了方便用户了解已填写的个人信息，路特斯科技从实用性角度出发，设计了**个人信息下载功能**。用户可将自己的账户信息导出至邮箱。

界面信息脱敏

为更好地保护用户个人隐私，尽可能防止数据泄漏，路特斯科技在手机App端对用户数据进行**脱敏后展示**，若用户需要查看完整信息，**需要通过手机验证码验证方可查看。**

3.2.11 其他实践活动

法律法规符合性管理实践

- ✓ 路特斯科技通过法律法规符合性的有效管理，有效识别和主动防范、管理和处置数据安全与隐私保护问题，避免违反数据安全与隐私保护相关的法律、法规、规章及合同要求

数据安全与隐私保护法律法规清单

- ✓ 路特斯科技整理了数据安全与隐私保护相关的国际公约、中国法律法规以及业务开展国法规（包括欧洲、美国、英国等）
- ✓ 确保更好地满足各地区对数据安全和隐私保护的要求
- ✓ 不断完善数据安全与隐私保护管理体系，保障数据安全合规

隐私合规管控表

- ✓ 个人信息盘点：记录了采取的安全措施（包括组织措施、技术措施等）以及个人信息的处置情况
- ✓ 个人信息处理活动：记录了个人信息在数据生命周期中的情况，并将数据出境和可能发生的安全事件纳入其中

云安全管理实践

- ✓ 路特斯科技通过从账号管理、网络架构、云基础配置、云产品防护、云应用系统、云审计六个方面规范了路特斯科技云资源的管理和使用

第四章

未来发展趋势展望

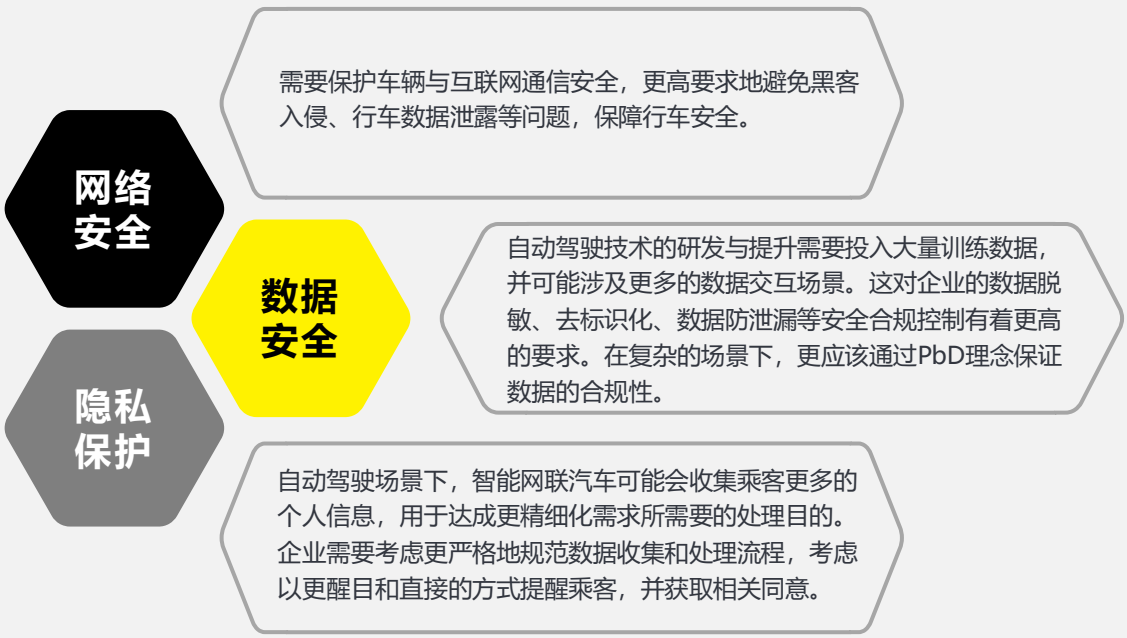
本章展望了智能网联汽车行业在数据安全合规领域的发展趋势。

智能网联汽车高速发展，用户基数快速增长，技术发展日新月异，在数据安全合规领域带来了新的挑战与机遇，需要行业参与者共同关注：

1 新技术的使用会引入新的安全合规风险

随着云、AI、5G等技术快速走向成熟商用，智能网联汽车行业正在不断催生新产品、新服务，例如自动驾驶。新服务对海量数据的处理能力的需求推动了全行业数据使用技术的进步。

随之而来的是由于引入新技术而增大的风险暴露面。自动驾驶作为监管关注的重点领域，也面临着全生态链的安全与合规挑战，也是智能网联汽车行业企业未来的数据安全与合规重点：



2 消费者比以往更加关注数据安全合规问题

消费者感知的个人信息保护合规，除了智能网联汽车使用相关的数据合规，还包括企业在服务周期内提供服务过程中的隐私保护合规性。作为终端用户，消费者在享受基于个人信息处理的服务时，希望可以充分实现自身数据主体权利，避免个人信息违规使用。这要求企业更严格地执行数据安全合规管控，在所有新业务场景都充分评估数据使用的合规性，以确保车主权益得到保护。

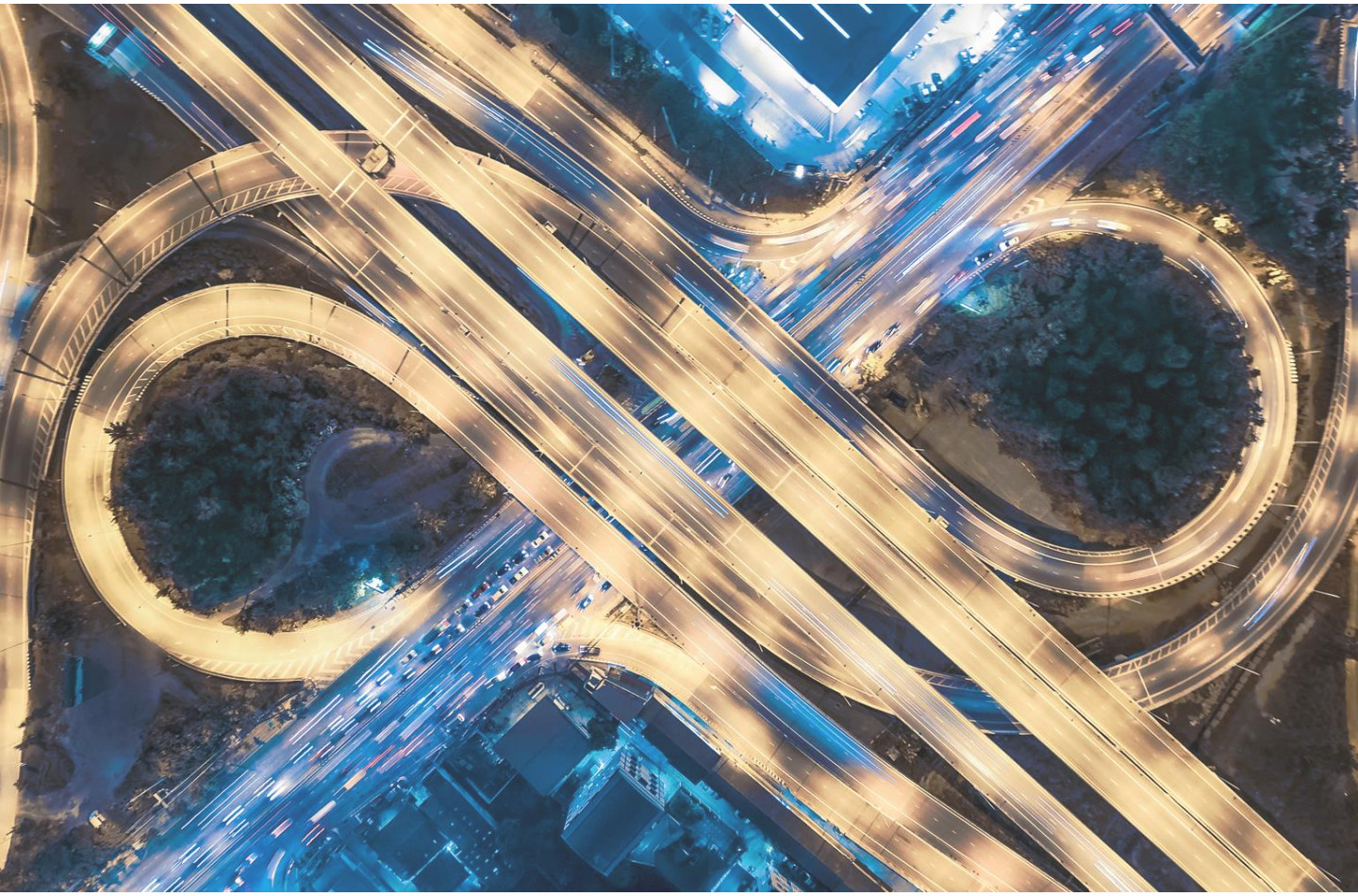
企业赢得消费者信任，需要从全公司发展战略层面入手，确保数据全生命周期的合规性，并持续投入数据安全合规领域。

合规能力正逐渐成为品牌竞争力的一部分。数据安全合规，特别是隐私合规已成为消费者关注重点。良好的数据安全合规实践有助于企业赢得用户信任，获取商业竞争优势，保持业务的可持续发展。

3 全球智能网联汽车数据监管趋势

随着信息基础设施的建设加速，智能网联汽车提供的服务更加丰富，车与车、车与人、车与云之间的数据交互需求随之不断增长。与传统汽车相比，智能网联汽车业务发展与服务构建的方式均已转向数据驱动。同时，全球日益严格的数据监管使企业在业务创新过程中必须对数据使用的合规性进行充分的论证与保障。

目前智能网联汽车的数据合规监管趋向各场景不断细化，监管部门、数据处理者及数据处理活动的相关方均有明确的职责。可预见未来行业内企业仍需对数据使用监管动态保持关注，根据数据使用场景匹配合规要求，及时调整安全合规控制，以保持持续合规，确保业务健康发展。



附录

地区	名称	类别
欧洲	《通用数据保护条例》（General Data Protection Regulation，GDPR）	法律法规
	《网络安全法案》（Cybersecurity Act）	法律法规
	《通用安全法规》（European General Safety Regulation, GSR）	法律法规
	《车联网个人数据保护指南 v2.0》（Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications）	行业规范
英国	《自动与电动汽车法案》（Automated and Electric Vehicles Act 2018）	法律法规
	《2018数据保护法案》（Data Protection Act 2018, DPA 2018）	法律法规
	《联网和自动驾驶车辆网络安全重要原则》（The Key Principles of Cyber Security for Connected and Automated Vehicles）	行业规范
美国	《美国数据隐私和保护法案》（H.R.8152 - American Data Privacy and Protection Act, ADPPA）	法律法规
	《加州消费者隐私法案》（California Consumer Privacy Act，CCPA）	法律法规
	《加利福尼亚隐私权法案》（CPRA, CCPA修正版）（California Privacy Rights Act, “CPRA”, also referred as “CCPA, as amended”）	法律法规
	《自动驾驶法案》（H.R. 3388 - SELF DRIVE Act）	法律法规
	《自动驾驶汽车启动法案》（S.1885 - AV START Act）	法律法规
	《现代车辆安全性的网络安全最佳实践》（Cybersecurity Best Practices for the Safety of Modern Vehicles）	行业规范
中国	《网络安全法》	法律法规
	《数据安全法》	法律法规
	《个人信息保护法》	法律法规
	《数据出境安全评估办法》	法律法规
	《数据出境安全评估申报指南（第一版）》	法律法规
	《汽车数据安全管理若干规定（试行）》	法律法规
	《工业和信息化部关于加强车联网网络安全和数据安全工作的通知》	法律法规
	《信息安全技术 汽车数据处理安全要求》（GB/T 41871-2022）	行业规范
	《车联网信息服务 用户个人信息保护要求》（YD/T 3746-2020）	行业规范
	《车联网信息服务 数据安全技术要求》（YD/T 3751-2020）	行业规范
	《车联网信息服务平台安全防护技术要求》（YD/T 3752-2020）	行业规范
	《智能网联汽车 数据通用要求》（征求意见稿）	行业规范
通用	ISO/IEC 27001 信息安全管理体系	行业规范
	ISO/IEC 27701 隐私保护体系	行业规范
	《网络安全管理系统 》(UN R155)	行业规范
	《软件更新管理系统 》(UN R156)	行业规范
	ISO/IEC 27018 云隐保护认证	行业规范
	ISO/SAE 21434 《道路车辆-信息安全工程》	行业规范

编写指导：

路特斯科技

首席信息官 臧宏念

质量负责人 Mahaendra Ibrahim Gofar

普华永道中国

网络安全及隐私服务合伙人 万彬

主编人员：

路特斯科技

熊吉

刘志良

戴悠悠

卢小溪

贾卓

徐晓萌

周丹

普华永道中国

楼耸

郑奕君

何欣晟

李佳秀

丁晓宇

感谢北京大成律师事务所对本白皮书成文的贡献

吴沈括

孙鹏程

赵中星

沈鑫瑶